## 3321 ACCEPTABLE USE OF COMPUTER NETWORK(S)/COMPUTERS AND RESOURCES BY TEACHING STAFF MEMBERS

The Board recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred that those changes will alter the nature of teaching and learning. Access to telecommunications will allow teaching staff members to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The Board supports access by teaching staff members to information sources but reserves the right to limit in-school use to materials appropriate to educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes that telecommunications will allow teaching staff members access to information sources that have not been pre-screened using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer network(s) and declares unethical, unacceptable, inappropriate or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, instituting legal action or taking any other appropriate action as deemed necessary.

The Board provides access to computer network(s)/computers for administrative and educational purposes only. The Board retains the right to restrict or terminate teaching staff member’s access to the computer network(s)/computers at any time, for any reason. The Board retains the right to have the Superintendent or designee monitor network activity, in any form necessary, to maintain the integrity of the network(s) and ensure its proper use. No employee or other individual has any expectation of privacy related to his/her use of the computer network.

Standards for Use of Computer Network(s)

Any individual engaging in the following actions declared unethical, unacceptable or illegal when using computer network(s)/computers shall be subject to legal and/or disciplinary action:

1. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities which violate federal, state, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the network(s). Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles and/or communication vehicles used in the work environment.

2. Using the computer network(s)/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

3. Using the computer network(s) in a manner that:

    a. Intentionally disrupts network traffic or crashes the network;

    b. Degrades or disrupts equipment or system performance;

    c. Uses the computing resources of the school district for commercial purposes, financial gain or fraud;

    d. Steals data or other intellectual property;

    e. Gains or seeks unauthorized access to the files of others, or impedes access to, disrupts or changes the data of another user;

    f. Gains or seeks unauthorized access to resources or entities;

    g. Forges electronic mail messages or uses an account owned by others;

    h. Invades privacy of others;

    i. Posts anonymous messages;

    j. Possesses any data which is a violation of this policy; and/or

    k. Engages in other activities that do not advance the educational purposes for which computer network(s)/computers are provided.

Violations

Individuals violating this policy shall be subject to appropriate disciplinary actions as defined by Policy No. 3150, Discipline which includes but are not limited to:

1. Use of the network(s)/computers only under direct supervision;

2. Suspension of network privileges;

3. Revocation of network privileges;

4. Suspension of computer privileges;

5. Revocation of computer privileges;

6. Suspension;

7. Dismissal;

8. Legal action and prosecution by the authorities; and/or

9. Any appropriate action that may be deemed necessary as determined by the Superintendent and approved by the Board of Education.

User Agreement and Code of Conduct for Technology Use at Ridgewood Public Schools

Ridgewood Public Schools (RPS) maintains and makes available technology to pupils and faculty for a wide range of applications. All users of the RPS's equipment and software are reminded that technology access comes with responsibility. The district's technology resources are expected to be used exclusively for education-related purposes. Users need to know that they have no expectation of privacy with respect to all stored files, including email files.

By logging on to the school's network computer, the user indicates acceptance of the policy set forth below in this document.

Access to Network

- Access to RPS's computers is provided to the school community as a tool to complete school related projects and assignments. Personal computers are not allowed to be connected to our data network.

- Users must keep passwords secure.

Software Installation and Use

- Users may not install software of any type, including games, to computers or to the school's network. Only software licensed to the school and approved by the Director of MIS Department may be used.

- Deletions, additions or any modifications to the Windows or Macintosh computer are not allowed. Users may not modify or damage any hardware, software application or operating system settings that would change the appearance or operation of the computers or network.

Ethical Use of Technology Resources

- Users must respect copyright laws. Plagiarism in any form will not be tolerated. This applies to all forms of print and digital media including but not limited to: electronic encyclopedias, image files, sound and video files. Proper citations and credits must be included where appropriate.

- While using the Internet, users must follow the accepted rules of network etiquette and conduct themselves in a responsible; ethical and polite manner. Users may not transmit, receive, submit, or publish any defamatory, abusive, obscene, threatening or potentially dangerous content. Any user encountering such material whether intentionally or not must notify a teacher or supervisor immediately. If no one is available at the time, the user is obligated to log off the network, and then notify a teacher or supervisor as soon as possible.

- Usage may be monitored to insure that users do not engage in inappropriate or illegal activity.

- Staff supervising pupils must ensure that the district's resources are used ethically and responsibly.

  - Optical scanners, camera, video equipment, external storage devices and other peripherals are provided for school related activities.

  - Users will minimize the use of the printers and print only school-related materials.

- All users must respect the work of other pupils and faculty by not accessing, copying, modifying or deleting the files of others.

- Any malicious attempt to harm or destroy district equipment, software, materials and/or data is prohibited.

Email

- School staff is provided with unique email accounts and are expected to use this account for their communication. Users need to know that the Ridgewood Public Schools may restrict access to personal email accounts.

- Pupils are not provided with school email accounts.

Additional Guidelines

- Food or drink should not be brought into computer labs or near computers.

- Users are personally responsible for making backups of any data files stored on their local hard drive or to their designated network personal folder.

Violation of any of the above policy shall result in administrative and/or legal disciplinary actions that include but are not limited to removal of all computer privileges.

N.J.S.A. 2A:38A-3

Adopted: 7 December 2009